UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/764,483	01/27/2004	Gun-il Lee	1793.1183	6277

21171 7590 06/22/2009

STAAS & HALSEY LLP
SUITE 700
1201 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
NGUYEN, ALLEN H	

ART UNIT	PAPER NUMBER
2625	

MAIL DATE	DELIVERY MODE
06/22/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/764,483	LEE, GUN-IL	
	Examiner	Art Unit	
	Allen H. Nguyen	2625	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 March 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *6-11* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *6-11* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 January 2004* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

- This office action is responsive to the following communication: Amendment filed on 03/06/2009.
- Claims 6-11 are currently pending in the application.

Response to Arguments

1. Applicant's arguments filed 03/06/2009 have been fully considered but they are not persuasive.

2. With respect to applicant's arguments that "Berkema does not obviate the technical feature of claim 6 where the security information is directly transmitted via a security communication line different from a communication line that transmits the document data from the transmitting facsimile machine to the receiving facsimile machine".

In reply: Debry '728 does not explicitly show wherein the security information is directly transmitted via a security communication line different from a communication line that directly transmits the document data from the transmitting machine to the receiving machine.

However, the above-mentioned claimed limitations are well known in the art as evidenced by Yajima '833. In particular, Yajima '833 teaches wherein the security information is directly transmitted via a security communication line (i.e., the identification data is automatically transmitted from the portable phone 1 to the printer 3; see page 4, paragraph [0055], fig. 1) different from a

communication line that directly transmits the document data from the transmitting machine to the receiving machine (i.e., a data transmitting/receiving section 11 to perform data communications with the portable phone 1; see page 3, paragraph [0047], fig. 1).

In view of the above, having the system of DeBry and then given the well-established teaching of Yajima, it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the system of DeBry as taught by Yajima to include: wherein the security information is directly transmitted via a security communication line different from a communication line that directly transmits the document data from the transmitting machine to the receiving machine, since Yajima stated on page 1, paragraph [0005] that such a modification would be allowing to securely provide the printed matter produced according to the specific print job to the user who directed the print job.

Drawings

3. The drawings are objected to under 37 CFR 1.83(a). The drawings must show every feature of the invention specified in the claims. Therefore, the limitation of "transmitting the security information directly to the receiving facsimile machine from the transmitting facsimile machine in fig. 3" must be shown or the feature(s) canceled from the claim(s). No new matter should be entered.

Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 6-11 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim 6 contains subject matter which was not described in the specification in such a way as to

reasonably convey to one skilled in the relevant art that the inventor, at the time the application was filed, had possession of the claimed invention.

1. Claims 6-11 are also rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

Regarding claim 6, the claim requires "the method comprising: transmitting the security information and the document data directly to the receiving facsimile machine from the transmitting facsimile machine" which was not described, in the specification or figure 3, in such a way as to reasonably convey to one skilled in the relevant art that the inventor, at the time the application was filed, had possession of the claimed invention. Figure 3 shows that the security information is located at the security server 250, it is not possible for the security information stored in the security server 250 to magically appear at the transmitting facsimile machine 220 and later directly transmitted with the document to the receiving facsimile machine 240.

Regarding claims 7-11, claims 7-11 are rejected under 35 U.S.C. 112, first paragraph, as being depend on rejected base claims.

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 6-11 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claim 6, the limitations of "the method comprising: storing the security information on the security server; and transmitting the security information and the document data directly to the receiving facsimile machine from the transmitting facsimile machine" are the limitations" as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. It is not clear for the security information stored in the security server 250 to magically appear at the transmitting facsimile machine 220 and later directly transmitted with the document to the receiving facsimile machine 240.

Regarding claims 7-11, claims 7-11 are rejected under 35 U.S.C. 112, second paragraph, as being depend on rejected base claims.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which

said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 6-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over DeBry (US 6,385,728) in view of Yajima et al. (US 2002/0016833).

Regarding claim 6, DeBry '728 discloses a method (Figs. 1, 5) of selectively printing document data (Document Source 10, fig. 1) using a security server (Certificate Authority 60, fig. 4) for machines (User 20 / Print System 30, fig. 4), which provides security information on users (i.e., a certificate authority 60 to authenticate the user's digital certificate; Col. 9, lines 19-20) who are authorized to print document data transmitted from a transmitting facsimile machine (i.e., a fax machine may be understood to be a network printer; Col. 12, line15-20, fig. 3, Print Server 30) to a receiving machine (i.e., since a facsimile machine may be understood to be a printer, the Print System 30 transmitted the document to the user' computer 20, and user's computer 20 received the document from the Print System 30. Therefore, user's computer 20 or client's computer is a receiving facsimile machine and the user is authenticated at the user's machine 20; Col. 9, lines 35-40 and col. 12, lines 20-25, fig. 4) to the receiving machine (The User / Client 20, fig. 3), the method comprising:

storing the security information on the security server (i.e., the authority 60 includes a public key in the certificate given to the printer and encodes the corresponding private key with the secret key from the database; Col. 9, lines 63-65);

transmitting the security information (i.e., the printer may then send, 402, the public key and user identification to a certificate authority 60 to authenticate the user's digital certificate. The print system now has the user's public key and knows that it is authenticated. The printer sends, 403, to the user a random message; See col. 9, lines 18-23, fig. 4) and the document data directly (Document is spooled 525, files are transmitted directly between the sender and the intended user; col. 4, lines 40-45 , fig. 5) to the receiving machine (User 20, fig. 4) from the transmitting machine (Print System 30, fig. 4);

receiving user information on a user attempting to print the document data (i.e., the user encrypts the message with its private key and sends, 404, it back to the printer; Col. 9, lines 23-24) at the receiving facsimile machine (User 20, fig. 4);

authenticating the user based on a result of comparing the received user information with the security information (i.e., the print system decrypts the message with the user's public key. If it matches the original message, then the printing system knows that the user is who the user purports to be; Col. 9, lines 24-27);

printing the document data if the user is authenticated at the receiving machine (i.e., since a facsimile machine may be understood to be a printer, the Print System 30 transmitted the document to the user' computer 20, and user's computer 20 received the document from the Print System 30. Therefore, user's computer 20 is a receiving facsimile machine and the user is authenticated at the user's machine 20; Col. 9, lines 35-40 and col. 12, lines 20-25, fig. 4),

Debry '728 does not explicitly show wherein the security information is directly transmitted via a security communication line different from a communication line that directly transmits the document data from the transmitting machine to the receiving machine.

However, the above-mentioned claimed limitations are well known in the art as evidenced by Yajima '833. In particular, Yajima '833 teaches wherein the security information is directly transmitted via a security communication line (i.e., the identification data is automatically transmitted from the portable phone 1 to the printer 3; see page 4, paragraph [0055], fig. 1) different from a communication line that directly transmits the document data from the transmitting machine to the receiving machine (i.e., a data transmitting/receiving section 11 to perform data communications with the portable phone 1; see page 3, paragraph [0047], fig. 1).

In view of the above, having the system of DeBry and then given the well-established teaching of Yajima, it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the system of DeBry as taught by Yajima to include: wherein the security information is directly transmitted via a security communication line different from a communication line that directly transmits the document data from the transmitting machine to the receiving machine, since Yajima stated on page 1, paragraph [0005] that such a modification would be allowing to securely provide the printed matter produced according to the specific print job to the user who directed the print job.

Regarding claim 7, DeBry '728 discloses the method, wherein the security information includes at least a plurality of identifications and passwords of the authorized users (i.e., access to resources of a computer system ("server") from another system or user ("user") has been controlled through passwords. This requires the server to maintain a database of all authorized users and each user's password; Col. 4, lines 15-20).

Regarding claim 8, DeBry '728 discloses the method, wherein the authenticating the user (User 20, fig. 4) based on a result of comparing the received user information (Digital Certificate, fig. 4) with the security information (Authenticates Certificate 402, fig. 4) comprises:

providing the received user information to the security server (i.e., in a certificate-based access control system, the server only needs to authenticate certificates issued by a certification authority; Col. 4, lines 22-24) for the facsimile machines (i.e., a fax machine may be understood to be a printer; see col. 12, lines 15-22);

enabling the security server for the facsimile machines to determine whether to authenticate the unauthorized user based on a result of comparing the received user information with the security information and to inform the receiving facsimile machine of a result of the determination (i.e., to gain access to resources of the server, the user submits the user's certificate. From the certificate, which contains data that cannot be forged, the server can obtain the

user's authenticated public number, personal data, and access privileges. The server can then transmit to the user a random message that the user must digitally sign with the user's private number and return it to the server. The server can then authenticate the digital signature using the public number in the certificate and check that the signed message is the same it sent to the user. With this digitally-signed response, the server can determine if the user has the correct private number corresponding to the authenticated public number in the certificate; See col. 4, lines 25-40).

Regarding claim 9, DeBry '728 discloses the method, wherein the authenticating the user (User 20, fig. 4) based on a result of comparing the received user information (Digital Certificate, fig. 4) with the security information (Authenticates Certificate 402, fig. 4) comprises:

providing the received user information to the transmitting facsimile machine (i.e., the Print System 30 can obtain the user's authenticated public number, personal data, and access privileges; Col. 4, lines 28-30);

enabling the transmitting facsimile machine (i.e., a fax machine may be understood to be a printer; Col. 12, lines 15-22, fig. 4, Print System 30) to determine whether to authenticate the unauthorized user or not based on a result of comparing the received user information with the security information and to inform the receiving machine (User/Client 20, fig. 4) of a result of the determination (i.e., a user 20/Receiving Machine will request the document from the Print System 30, the Print System will verify that the user has the correct

access privileges, and if so, then the Print System will send a copy of the document to the user; col. 4, lines 50-55).

Regarding claim 10, DeBry '728 discloses the method, wherein the authenticating the user (User 20, fig. 4) based on a result of comparing the received user information (Digital Certificate, fig. 4) with the security information (Authenticates Certificate 402, fig. 4) comprises:

providing the received user information to the receiving machine (i.e., the Print System 30 can transmit to the user a random message that the user must digitally sign with the user's private number and return it to the Print server; Col. 4, lines 30-32, fig. 4);

enabling the receiving facsimile machine (i.e., since a facsimile machine may be understood to be a printer, the Print System 30 transmitted the document to the user' computer 20, and user's computer 20 received the document from the Print System 30. Therefore, user's computer 20 is a receiving facsimile machine and the user is authenticated at the user's machine 20; Col. 9, lines 35-40 and col. 12, lines 20-25, fig. 4) to determine whether to authenticate the unauthorized user or not based on a result of comparing the received user information with the security information and to inform the receiving machine of a result of the determination (i.e., the server can authenticate the digital signature using the public number in the certificate and check that the signed message is the same it sent to the user. With this digitally-signed response, the server can

determine if the user has the correct private number corresponding to the authenticated public number in the certificate).

Regarding claim 11, DeBry '728 discloses a computer-readable medium encoded with processing instructions implementing the method (i.e., having computer-readable program code, may be embodied within one or more computer-usable media such as memory devices or transmitting devices, thereby making a computer program product; Col. 11, lines 20-25) of selectively printing document data (File Source 10, fig. 3) using a security server (Certificate Authority 60, fig. 4), which provides security information on users who are authorized to print document data transmitted from a transmitting facsimile machine (i.e., a fax machine may be understood to be a printer; Col. 12, line19-20, fig. 3, Print Server 30) to a receiving facsimile machine (User/Client 20, fig. 3), to the receiving facsimile machine (i.e., since a facsimile machine may be understood to be a printer, the Print System 30 transmitted the document to the user' computer 20, and user's computer 20 received the document from the Print System 30. Therefore, user's computer 20 is a receiving facsimile machine and the user is authenticated at the user's machine 20; Col. 9, lines 35-40 and col. 12, lines 20-25, fig. 4).

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Fischer (US 5,005,200) discloses public key/signature cryptosystem with enhanced digital signature certification.

Davis et al. (US 5,633,932) discloses apparatus and method for preventing disclosure through user-authentication at a printing node.

Baba (US 7,304,755) discloses facsimile apparatus, a method of displaying advertisement information through the facsimile apparatus and a communication system provided with the facsimile apparatus.

10. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Allen H. Nguyen whose telephone number is (571)270-1229. The examiner can normally be reached on 9:00 AM-6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, KING Y. POON can be reached on (571) 272-7440. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/King Y. Poon/
Supervisory Patent Examiner, Art Unit 2625

/Allen H. Nguyen/
Examiner, Art Unit 2625